

**INFORMATION TECHNOLOGY:
The Bureau of the Public Debt's Certificate
Policy Statement Should Be Updated**

OIG-03-009

October 24, 2002



Office of Inspector General

The Department of the Treasury

Contents

Audit Report	2
Results in Brief.....	3
Background	4
Results and Recommendation	5
The Certificate Policy Statement Should Be Updated To Effectively Manage Public Key Infrastructure	5

Appendices

Appendix 1:	Objective, Scope, and Methodology	7
Appendix 2:	Glossary	8
Appendix 3:	Management Comments.....	9
Appendix 4:	Major Contributors To This Report	10
Appendix 5:	Report Distribution.....	11

Abbreviations

BPD	Bureau of the Public Debt
CA	Certificate Authority
CP	Certificate Policy
CPS	Certificate Policy Statement
PKI	Public Key Infrastructure
SPSS	Special Purpose Securities System
Treasury	Department of the Treasury

*The Department of the Treasury
Office of Inspector General*

Van Zeck, Commissioner
Bureau of the Public Debt

The Office of Inspector General's (OIG) Annual Audit Plan for Fiscal Year 2001 included the audit, *Treasury Bureaus' Smart Card and Public Key Infrastructure Implementation*. The OIG's management uses the Annual Audit Plan as a means to identify and assign available resources to high priority areas consistent with the Department of the Treasury (Treasury) and bureau level strategic plans, as well as other high-risk areas.

Public Key Infrastructure (PKI) technology can facilitate and simplify the delivery of products and services by providing electronic approaches to processes that have been historically paper-based. These electronic solutions support the integrity of data and rely on authentication and encryption techniques to ensure privacy.

The Bureau of the Public Debt's (BPD) PKI technology includes a combination of hardware and software services, and encryption technologies. The BPD's PKI technology integrates digital certificates, public key cryptography, and certification authorities into a completely networked security architecture. The implementation of PKI is dependent on policies, procedures, and human resources to provide a secure electronic delivery operation and protect sensitive communications and transactions.

The overall objective of this audit was to determine whether BPD is effectively managing the implementation of PKI. During the audit, we reviewed policies and procedures for PKI, including BPD's Certificate Policy Statement (CPS). We also reviewed BPD's PKI pilots and published standards. A more detailed description of our objective, scope, and methodology is provided in Appendix 1.

Results in Brief

During our audit, we identified that BPD has not developed all the documentation needed to effectively manage its PKI. Though BPD has made a significant effort in leading Treasury's PKI initiatives, we found that the CPS for PKI does not consistently and adequately support current operations. These concerns increase the risk that security controls associated with BPD's PKI can be circumvented and jeopardize the integrity of web transactions.

Our report includes a recommendation that, in our opinion, will assist BPD in addressing the deficiency we identified. Specifically, we are recommending that the Commissioner, BPD, ensure that the CPS is updated to adequately support PKI.

In its response to our draft report, BPD concurred with our results and recommendation. The bureau has already commenced efforts to implement our recommendation. The BPD's response is summarized and evaluated in the body of this report and included, in detail, in Appendix 3, Management Comments.

Background

A PKI is defined as an information technology infrastructure that enables users of an unsecured, public network (such as the Internet) to securely and privately exchange data through the use of a public and private cryptographic keys. These keys are obtained and shared through a trusted authority, known as the Certificate Authority (CA). The use and proper management of PKI technology will provide organizations with the ability to secure interactions over the Internet and other open networks.

In 1997, BPD made a decision to use a CA to authenticate its customer base for its Special Purpose Securities System (SPSS), which was placed into production in December of 1999. The BPD's PKI is currently classified as a general support system for SPSS. The SPSS provides an interactive Internet interface for users, allowing them to submit transactions and manage their accounts, using public key technology.

With this technology, web server certificates are issued to authenticate and protect the integrity of transactions performed over the Internet. All internal BPD web-based applications use web server certificates issued by BPD's PKI.

The following table provides a historical background of BPD's PKI Implementation.

Table 1: History of BPD's Implementation

Decision to use a CA to authenticate customers	December 1997
Decision to restructure and build a fully functional PKI	October 1998
BPD's CPS finalized	April 1999
First application to use PKI - SPSS	December 1999

Results and Recommendation

The Certificate Policy Statement Should Be Updated To Effectively Manage Public Key Infrastructure

Though BPD has developed a CPS, we determined that the statement has not been updated to include the conduct of third party reviews or audits to identify whether discrepancies exist in CA operations. This documentation is needed for BPD to effectively manage its PKI technology and ensure web transactions are secure.

The purpose of a CPS is to define the practices and procedures that the CA utilizes in conducting services and operations. A CPS also provides the detailed procedures users rely on to secure transactions conducted over the Internet. Treasury's Security Manual requires all CAs to operate under a CPS that provides guidance for the performance of third party reviews or audits.

Without the detailed procedures needed to conduct reviews, BPD cannot ensure sufficient controls are in place to appropriately issue, manage, and revoke certificates. A lack of controls could bring the reliability of BPD's PKI into question. Customers rely on the trustworthiness that comes with the CA's issuance and maintenance of certificates to secure transactions over the Internet. The ineffective or improper management of PKI could pose weaknesses and serious risks to the overall integrity of BPD's CA, the services it provides, and the use of PKI technology.

Recommendation

The Commissioner, BPD, should update its CPS to include procedures for the performance of third party reviews and audits.

Management Response:

The BPD concurred with the recommendation and will update its CPS. A revised CPS has already been drafted and is currently under final review by BPD's Chief Counsel's Office. The BPD expects to publish its new CPS by December 31, 2002.

OIG Comment:

The OIG agrees that the formal steps BPD management is taking will satisfy the intent of the recommendation.

* * * * *

We would like to extend our appreciation to the BPD for the cooperation and courtesies extended to our staff during the review. If you have any questions, please contact me at (202) 927-5007, or Angela Payton, Computer Specialist, Office of Information Technology Audit, at (202) 927-5015. Major contributors to this report are listed in Appendix 4.

/s/

Edward G. Coleman

Director, Office of Information Technology Audits

The overall objective of this audit was to determine whether BPD's PKI implementation is effectively managed. This objective was accomplished by determining whether BPD has policies, procedures, and management controls in place to ensure reasonable assurance that the implementation of PKI technology provides adequate system security and data integrity.

The audit was conducted in accordance with generally accepted auditing standards. The scope of our audit did not include testing PKI controls or the integrity of data. This report details the fieldwork performed at BPD's Information Technology Data Center between May and June 2002.

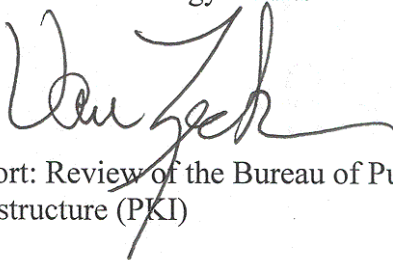
Authentication	A process used to confirm the identity of a person or to prove the integrity of specific information.
Certificate	A message stating that a public key belongs to or is associated with a given individual, organization, or device. The party issuing the certificate is a certificate authority, and the party receiving it is called the subscriber. The digital signature on a certificate provides assurance of the origin of the CA signing it and that the certificate has not been tampered with since issuance.
Certificate Authority	An entity that signs, issues, and manages public key certificates.
Private Key	A mathematical key (kept secret by the holder) used to create digital signatures and, depending upon the algorithm, to decrypt messages or files encrypted (for confidentiality) with the corresponding public key.
Public Key	A mathematical key that can be made publicly available and used to verify signatures created with its corresponding private key. Depending on the algorithm, public keys can also be used to encrypt messages or files that can then be decrypted with the corresponding private key.



DEPARTMENT OF THE TREASURY
BUREAU OF THE PUBLIC DEBT
PARKERSBURG, WV 26106-1328

October 15, 2002

MEMORANDUM TO: Edward G. Coleman
Director, Information Technology Audits

FROM: Van Zeck
Commissioner 

SUBJECT: Draft Audit Report: Review of the Bureau of Public Debt's
Public Key Infrastructure (PKI)

In response to your October 02, 2002 draft audit report, the following comments are offered:

Public Debt agrees with your recommendation to update its Certificate Practice Statement (CPS) and has already drafted a revised CPS, currently under final review by our Chief Counsel's Office. We expect to publish this new CPS no later than 12/31/02. This should close the finding noted in your draft audit report.

We appreciate your acknowledgement of the leading role Public Debt has played in Treasury's PKI initiatives, but we respectfully disagree with your comment in the report that "BPD cannot ensure sufficient controls are in place to appropriately issue, manage, and revoke certificates." We have effectively managed our certificates for several years and have other procedures in place that mitigate the few omissions in the current CPS. We do plan to implement the new CPS to bring us into full compliance with the Treasury Security Manual.

Thank you for the opportunity to comment on this draft report.

Office of Information Technology Audits

Edward Coleman, Director
Barbara Bartuska, Audit Manager
Patrick Nadon, Audit Manager
Sharell Matthews, IT Auditor
Anthony Nicholson, IT Auditor
Angela Payton, Computer Specialist

Bureau of the Public Debt

Commissioner, Bureau of the Public Debt
Assistant Commissioner, Office of Information Technology

Treasury

Office of the Deputy Assistant Secretary for Information
Systems/Chief Information Officer
Office of Accounting and Internal Control

OMB

Office of Inspector General Budget Examiner